IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. JAMES GORDON MEEK *Defendant*.	Case No. 1:23-cr-65

UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM DROPBOX

The defendant moves this court to suppress evidence obtained from the search of his Dropbox account, arguing that the content was obtained in violation of his Fourth Amendment rights. As detailed below and supported by the attached declarations from the relevant parties, all searches of the defendant's account were conducted lawfully, and the defendant's argument fails at every step of the analysis. The motion to suppress should be denied.

RELEVANT BACKGROUND

The investigation into the defendant's criminal conduct began when Dropbox, Inc. ("Dropbox"), a cloud-based file storage system, identified five files of suspected child sexual abuse material (CSAM) located in the defendant's Dropbox account. On March 11, 2021, Dropbox submitted a CyberTip to the National Center for Missing and Exploited Children (NCMEC). Gov. Exh. 1 (CyberTip Report 87555105). Part A of this CyberTip indicated that Dropbox had detected five files containing child sexual abuse material (CSAM) in the defendant's Dropbox account, all of which had been "publicly shared" by the defendant and viewed in full by Dropbox prior to submission. *Id.* Part A of the CyberTip is generated by the information provided by Dropbox and cannot be changed by NCMEC. Gov. Exh. 6 (Declaration

of NCMEC Records Specialist Susan Lafontant).

NCMEC originally forwarded the CyberTip to the Virginia State Police (VSP), who identified the subscriber as residing in Arlington County and referred the case to the Arlington County Police Department (ACPD). Shortly thereafter, ACPD referred the case to the Federal Bureau of Investigation (FBI). After reviewing the CyberTip and associated files, the FBI drafted and submitted preservation requests to Dropbox, Google, and Skype on or about September 9, 2021. Gov. Exh. 2 (Declaration of Special Agent Richard Guida). The preservation request submitted to Google was drafted using a template and contained a typo mistakenly dating the letter as March 10, 2021. Gov. Exh. 3 (Declaration of Staff Operating Specialist Alexa George). However, the preservation requests were only sent after receipt of the CyberTip, as demonstrated by the declarations of SOS George and SA Guida, the automated email confirming receipt that Google sent to SOS George on September 9, 2021, Gov. Exh. 4 (Google Email Confirmation), and the dates on the requests to Dropbox and Skype.

Thereafter, the FBI proceeded to conduct its investigation, including the execution of a search pursuant to a warrant on the defendant's residence, where the government seized numerous electronic devices. A search of those devices revealed numerous images and videos of CSAM, as well as several instances of the defendant sending and receiving CSAM. Additional investigation revealed that while the defendant was not in the Eastern District of Virginia during some of the instances when he sent and received CSAM, he traveled back to the district shortly thereafter with CSAM on his phone. The defendant has been charged with one count of transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1); one count of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2); and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

On May 4, 2023, the defendant filed a motion to suppress evidence obtained from Dropbox. ECF No. 57.

ARGUMENT

The defendant's arguments are unsupported by the law or the facts of this case. First, the defendant has no standing to challenge the search of the CSAM files: because he voluntarily made those files public in his Dropbox account, he had no reasonable expectation of privacy in them. Second, even assuming that he *did* have a reasonable expectation of privacy in those publicly shared files, Dropbox conducted a lawful, private-party search of its own platform—motivated by its own independent business interest—and therefore did not act as a government agent. Third, the government did not exceed the scope of Dropbox's private search when the FBI reviewed the files previously reviewed by Dropbox. Fourth, the defendant has no property interest in the child sexual abuse material located within his Dropbox account. And finally, even if the Court were to determine that a Fourth Amendment violation occurred, suppression is unwarranted under the good faith exception.

A. The defendant lacks standing to assert that law enforcement conducted an unlawful search because he voluntarily shared the files with the public.

The Supreme Court has held that the person asserting that a search protected by the Fourth Amendment occurred must first "have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967). In challenging the alleged "search" of his publicly available files, the defendant bears the burden of establishing a reasonable expectation of privacy. *See, e.g., United States v. Daniels,* 41 F.4th 412, 415 (4th Cir. 2022) (quoting *United States v. Castellanos*, 716 F.3d 828, 833-35 (4th Cir. 2013) ("[T]o prevail in a fourth amendment challenge, the criminal defendant bears the burden of establishing a legitimate expectation of privacy in the

searched property, at the time of the search, by preponderance of the evidence.")). Absent such a showing, the defendant does not have standing to assert that law enforcement conducted an unlawful search or illegally seized objects. *See United States v. Barragan*, 379 F.3d 524, 529-30 (8th Cir. 2004).

Importantly, in *United States v. Jones*, 565 U.S. 400 (2012), the Court recognized that individuals do not have a reasonable expectation of privacy in information voluntarily conveyed to the public. *Id*. at 408-09. Similarly, courts addressing the issue of privacy in the peer-to-peer file sharing context have uniformly held there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file-sharing networks. *See*, *e.g.*, *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (per curiam); *United States v. Weast*, 811 F.3d 743, 747 (5th Cir. 2016); *United States v. Connor*, 521 Fed.Appx. 493 (6th Cir. 2013).

In this case, the defendant used Dropbox, "an online file syncing and collaboration service that allows users to access and share their files on computers, phones, tablets, and the Dropbox website." Gov. Ex. 5 (Declaration of Dropbox Content Safety Manager Tobi Wulff). As Dropbox explains, "[w]hen Dropbox users upload files to their Dropbox accounts, they can choose whether to keep files private within their accounts, to share their files with specified Dropbox users, *or to share their files with the public* by creating a 'shared link.' Files that are shared publicly can be accessed over the Internet by any person who knows the Uniform Resource Locator ("URL") for the shared link." *Id.* (emphasis added).

Critical to the analysis of whether the defendant had a reasonable expectation of privacy, the information Dropbox submitted in CyberTip Report 87555105 reflects that all five videos uploaded by the defendant were publicly shared. Gov. Exh. 1.[1] The defendant did not have an

[1] Dropbox even noted that the CSAM in question "was detected when a user attempted to create a shared link to the reported files or a shared link to a file containing the reported files." Gov. Exh. 5.

actual, subjective expectation of privacy because the defendant had already exposed the five files to the public—the exact opposite of exhibiting an expectation of privacy. *See United States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007) (noting an individual claiming a subjective expectation of privacy must demonstrate that he sought to preserve the objects of the search as private). The declaration from the Dropbox Content Safety Manager Tobi Wulff makes clear that the defendant shared those five files with the public, and thus he cannot claim the privacy protection of the Fourth Amendment.

B. Dropbox did not act as a government agent when it conducted a private search motivated by its own independent interest in removing CSAM from its platform.

Even if the Court determines that the defendant somehow *did* have an expectation of privacy in the publicly shared files, Dropbox acted independently and conducted the search in its capacity as a private party. The United States Supreme Court has consistently construed the Fourth Amendment's protection "as proscribing only governmental action." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)); *see also Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) (Fourth Amendment "does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative."). Therefore, a private party's search only implicates the Fourth Amendment if the party is "acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Ellyson*, 326 F.3d 522, 527–28 (4th Cir. 2003) (quoting *United States v. Jacobsen,* 466 U.S. at 113 (internal quotation marks omitted)).[2]

In undertaking the private search analysis, the Fourth Circuit has recognized two factors to be considered: (1) "whether the Government knew of and acquiesced in the private" individual's

[2] The defendant claims that the private search doctrine no longer provides an exception to the Fourth Amendment's warrant requirement after *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *See* Def. Mot. at 8. The defendant cites not one court that has even toyed with this proposition, much less adopted it. In fact, since *Carpenter* and *Riley* were decided, the Fourth Circuit has continued to embrace and apply the doctrine without hesitation. *See, e.g., United States v. Fall*, 955 F.3d 363, 370 (4th Cir. 2020) ("The private search doctrine is based on the principle that the Fourth Amendment does not protect against searches conducted by private individuals acting in a private capacity.").

challenged conduct; and (2) "whether the private individual intended to assist law enforcement or had some other independent motivation." *United States v. Day*, 591 F.3d 679, 683 (4th Cir. 2010) (quoting *Jarrett,* 338 F.3d at 344)). Because the government did not know of or acquiesce in Dropbox's search, and because Dropbox had a business motivation independent of assisting law enforcement in conducting its search, Dropbox was acting as a private actor, and its search does not implicate the Fourth Amendment.

I.) The government did not know of or acquiesce in Dropbox's private search.

In the instant case, the record makes clear that the government did not know of or acquiesce in Dropbox's conduct. There is no evidence that the government directly participated in Dropbox's independent search of its networks; in fact, the evidence demonstrates that Dropbox never directly communicated with law enforcement until September 2021, after it had discovered and reported the CSAM. Gov. Exh. 2 ("[T]he FBI had no coordination with Dropbox regarding this matter until on or about 09/09/2021 when the FBI served Dropbox with a preservation letter."); Gov. Exh. 5 ("Dropbox did not separately communicate with NCMEC or with law enforcement about the information provided in CyberTipline Report 87555105 before it was reported."). The only evidence the defendant cites to support his contention otherwise is a typographical error on a preservation request, which mistakenly indicated that the request was sent *to Google* (not even to Dropbox) prior to Dropbox's submission of the CyberTip, *see* Gov. Exh. 3, as well as the "date gap" between the last CSAM activity in the defendant's account and Dropbox's report. However, contrary to the defendant's suggestion, the time between these two dates does not indicate anything about whether the CSAM was located as part of a "routine" process. Furthermore, there is no requirement that Dropbox's search be "routine"—only lawful.

II.) Dropbox's search was motivated by its own, independent business interests.

Dropbox undoubtedly has a strong independent motivation to ensure that its platform

remains free of child sexual abuse material. In his declaration, Tobi Wulff, a Content Safety Manager at Dropbox, emphasizes that Dropbox "has a strong business interest in enforcing its Acceptable Use Policy and ensuring that its service is free of illegal content, including in particular CSAM. Gov. Exh. 5. To that end, Mr. Wulff continues, "Dropbox independently and voluntarily takes steps to safeguard our platform against CSAM because we do not want our services to be associated with or used to store such content, and because users may stop using our services if they encounter it." *Id.* Mr. Wulff further explains that "Removing CSAM from our services is thus critically important to protecting our users, our services, our brand, and our business interests." *Id.* As a private entity, Dropbox can lawfully search user content in an effort to protect that interest.[3]

In an analogous case involving AOL's private search of a defendant's email accounts for child pornography, the Fourth Circuit clearly held that that a provider's search of its own records for CSAM does "not equate to governmental conduct triggering constitutional protection." *United States v. Richardson*, 607 F.3d 357, 364 (4th Cir. 2010). This determination of private action has been continuously upheld in cases involving searches by other internet service providers like Dropbox: "Every court to consider the question—including the First, Fourth, Eighth, and Tenth Circuits—has concluded that an ISP's search of its own user's account does not implicate the Fourth Amendment." *United States v. Wolfenbarger*, No. 16-CR-00519-LHK-1, 2019 WL 6716357, at *24 (N.D. Cal. Dec. 10, 2019). *See also e.g., United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012); *Richardson*, 607 F.3d at 366-67 (4th Cir. 2010); *United States v. Stratton*, 229 F. Supp. 3d 1230, 1236-39 (D. Kan. 2017); *United States v. DiTomasso*, 81 F. Supp. 3d 304, 309-11 (S.D.N.Y. 2015); *United*

[3] The fact that 18 U.S.C. § 2258A imposes a requirement on electronic computing service providers like Dropbox to report apparent violations of 18 U.S.C. §§ 2252 and 2252A *once discovered* does not retroactively transform a service provider's search of user content into a government search. Notably, 18 U.S.C. § 2258A does not impose a requirement on Dropbox to search for apparent violations of 18 U.S.C. §§ 2252 and 2252A.

States v. Miller, No. 8:15CR172, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015); *United States v. Ackerman*, No. 13-10176-01-EFM, 2014 WL 2968164, at *5-6 (D. Kan. July 1, 2014), rev'd on other grounds, 831 F.3d 1292 (10th Cir. 2016); *United States v. Drivdahl*, No. CR-13-18-H-DLC, 2014 WL 896734, at *3-4 (D. Mont. Mar. 6, 2014); *United States v. Keith*, 980 F. Supp. 2d 33, 40-42 (D. Mass. 2013); *United States v. Rosenow*, No. 17CR3430 WQH, 2018 WL 6064949, at *9 (S.D. Cal. Nov. 20, 2018).

In the absence of evidence of government involvement in any of Dropbox's searches leading to its CyberTip report, and because Dropbox had its own interests to protect when finding and removing child sexual abuse material from its systems, it was not acting as a government agent when it conducted the challenged searches. There is no basis to suppress the information Dropbox gathered and subsequently provided to NCMEC.

C. The government did not exceed the scope of Dropbox's private search.

The defendant contends that the government exceeded the scope of Dropbox's search when (1) NCMEC reviewed the files, and (2) law enforcement reviewed the files. Both of these arguments are contradicted by the record.

As an initial matter, NCMEC is not a government agency, so the scope of its review is irrelevant to the Fourth Amendment analysis. As explained in NCMEC Records Specialist Susan Lafontant's declaration, "NCMEC is a private, non-profit corporation" whose "mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization." Gov. Exh. 6. NCMEC has operated the CyberTipline since 1998 "in furtherance of its private mission to serve as the national resource center and clearinghouse concerning online child sexual exploitation." *Id.* Moreover, law enforcement does not instigate or direct NCMEC in the processing of CyberTip reports and was not involved in NCMEC's opening and review of the flagged files in the present case. Therefore, NCMEC was not acting as a government agent when it opened and reviewed the

same files previously opened and viewed by Dropbox.

Even if this Court were to conclude that NCMEC is a government agent, NCMEC's search did not exceed the scope of Dropbox's private search—to the contrary, it was considerably more narrow than Dropbox's search. As detailed in Mr. Wulff's declaration, "[a]ll apparent child pornography is manually reviewed by a member of the Dropbox content safety team before it is reported to NCMEC…[w]hen Dropbox indicates in a CyberTipline report that a file was "Reviewed by ESP," or otherwise states or indicates that Dropbox has viewed or reviewed the file, Dropbox is referring to a review of that image by a human reviewer prior to making the report. Gov. Exh. 5. In contrast, upon receipt of the CyberTip, NCMEC staff reviewed only *two* of the five CSAM files previously reviewed by Dropbox, since the remaining three had hash values matching "files previously viewed and categorized as Apparent Child Pornography by NCMEC." Gov. Exh. 6. "The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Jacobsen*, 466 U.S. at 117-19 (holding that no search implicating the Fourth Amendment took place where the DEA agent did not discover anything in the suspicious package beyond what the FedEx employee had already found). Even if the Court finds that NCMEC is a government actor, there is no evidence that NCMEC's warrantless search exceeded the scope of Dropbox's private search, and the Fourth Amendment is not implicated. *See United States v. Stratton*, __ F.Supp. 3d __, No. 15-40084-01-DDC, 2017 WL 169041, at *7 (D. Kan. Jan. 17, 2017) (holding that there was no Fourth Amendment violation where NCMEC only looked at images that Sony had previously viewed because NCMEC's actions did not exceed the scope of Sony's private search); *Drivdahl*, 2014 WL 896734, at *4 (concluding that there was no Fourth Amendment violation where NCMEC only looked at images that Google had previously viewed because NCMEC's actions did not exceed the scope of Google's private search).

Similarly, the FBI did no more than review content already reviewed by Dropbox. Special Agent Guida evaluated the very same digital files Dropbox originally flagged and manually assessed through human review. Gov. Ex. 5. Agent Guida did not expand upon Dropbox's search. There is no evidence this initial search exceeded the scope of Dropbox's original investigation, and, therefore, the Fourth Amendment is not implicated.

D. The defendant has no property interest in the child sexual abuse material.

The defendant attempts to make a separate property interest argument, asserting that—even if the private search exception applies here and there is no violation of the defendant's *privacy* interest—the government violated the defendant's *property* interest in the Dropbox account and the CSAM videos. *See* Def. Mot. at 11-12. But the defendant has no property interest in unlawful videos depicting the sexual abuse of minors: "one cannot have a property right in that which is not subject to legal possession." *Cooper v. City of Greenwood*, 904 F.2d. 302, 305 (5th Cir. 1990).

Moreover, even assuming that the defendant had a property interest in child sexual abuse material, his argument applies the wrong framework to the Fourth Amendment analysis of an online account, such as the defendant's Dropbox account. In *Jones*, the Supreme Court noted that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis" relying on assessing the *privacy* interest. 565 U.S. at 411. "In the wake of *Jones*, the Supreme Court has routinely applied the *Katz* test, at the expense of the *Jones* test, to intrusions into cyberspace." *United States v. Weber*, 599 F.Supp.3d 1025, 1034 (D. Mont. 2022) (citing *Riley*, 573 U.S. at 378–403, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) (analyzing the warrantless inspection of cell phone data in terms of *Katz* privacy expectations, not *Jones* property intrusions); *Carpenter*, 138 S.Ct. at 2211–19 (analyzing law enforcement's obtainment of "historical cell phone records that provide a comprehensive chronicle of the user's past

movements" in terms of privacy expectations).

E. In the alternative, the good faith exception applies, and suppression is unwarranted.

Even if the Court holds that a Fourth Amendment violation occurred, the good faith exception to the Fourth Amendment's exclusionary rule, as set forth in *United States v. Leon*, 468 U.S. 897 (1984), applies here. In *Leon*, the Supreme Court explained, "[i]f the purpose of the [Fourth Amendment's] exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." 468 U.S. at 919 (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)). The exclusionary rule serves to deter "deliberate, reckless, or grossly negligent conduct." *Herring v. United States*, 555 U.S. 135, 144 (2009). Thus, to trigger the exclusionary rule, an officer's misconduct must be sufficiently deliberate that suppression could deter it; the court must also conclude that deterrence is worth the substantial cost of exclusion. *Id.* The test is whether "a reasonable, well-trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Brown*, 951 F.2d 999, 1004 (9th Cir. 1991) (internal citations omitted).

In this case, the FBI reviewed the CSAM files only after ensuring that Dropbox had already viewed those files. The process the FBI undertook in this case has been repeatedly upheld as lawful by courts, including the Fourth Circuit. *See, e.g., Richardson*, 607 F.3d at 364; *Stevenson*, 727 F.3d at 831; *Cameron*, 699 F.3d at 637-38. At the time the FBI conducted subsequent search warrants and investigation, the agents reasonably believed that Dropbox lawfully monitored its user's activities and lawfully reviewed these child sexual abuse material images before alerting NCMEC. They reasonably believed that NCMEC lawfully reviewed the information submitted by Dropbox and lawfully made the information available to law enforcement for their review. And because

courts have almost universally held that ISPs like Dropbox are not government entities (*see* Section B, *supra*), it was objectively reasonable for the agents to believe that Dropbox was not a government actor when they had no role in triggering Dropbox's search. For all of these reasons, the agents had a good faith belief that their review of the material was constitutional, and suppression is therefore unwarranted.

CONCLUSION

For the foregoing reasons, the defendant's motion to suppress should be denied.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/

Whitney Kramer
Special Assistant United States Attorney (LT)
Zoe Bedell
Assistant United States Attorney United States Attorney's Office
2100 Jamieson Ave.
Alexandria, Virginia 22314
Phone: 703-299-3700
Email: Whitney.Kramer@usdoj.gov